UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/681,870	10/08/2003	Saravanan Agasaveeran	CIS03-38(7401)	7379

22468 7590 01/11/2007 CHAPIN & HUANG L.L.C. WESTBOROUGH OFFICE PARK 1700 WEST PARK DRIVE WESTBOROUGH, MA 01581		

EXAMINER
HUSSAIN, TAUQIR

ART UNIT	PAPER NUMBER
2152	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

		Application No.	Applicant(s)
Office Action Summary		10/681,870	AGASAVEERAN ET AL.
		Examiner	Art Unit	
		Tauqir Hussain	2196	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *10/08/2003*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-27* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-27 are pending in this application.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claim 1-3, 5-8, 10-20, 22-24 and 27 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Scoredos et al. (Pub. No.: US 2004/0250127 A1), hereinafter

"Scoredos" in view of Reddy et al. (Patent No.: US 7062540 B2), hereinafter "Reddy".

4.   As to claim 1, Scoredos discloses, a method for filtering transport layer

connections with application layer information, comprising the steps of:

receiving a connection request having an application layer component and a

transport layer component ([0015, lines 1-4], where tcp/ip connection comprises of

transport layer component and application layer component.);

providing a connection database to store information about connection requests

([0016, lines 1-4], table of rules can be a database);

providing a throttle filter using data from the connection database, the throttle filter

to filter the connection request at the transport layer component ([0016, lines 1-5]);

applying the throttle filter to the received connection request ([0016, lines 8-9]);

if the throttle filter blocks the transport layer component of the connection

request, dropping the connection request silently ([0033, lines 2-4]); and

Scoredos does not explicitly disclose, providing a connection database to store

information about associated application layer outcomes; or if the throttle filter allows

the transport layer component of the connection request, proceeding with the

application layer component. However, Reddy teaches, providing a connection

database to store information of associated application layer outcomes (Col.7, lines 64-

66) ; and if the throttle filter allows the transport layer component of the connection

request, proceeding with the application layer component (Col.8, lines 5-23, where

notifications are outcome of applications outcome which are communicated through

firewall by web server and displayed at user interface in http form or could be a HTML

page with time out notice or error notice or status)

Therefore, it would have been obvious to one ordinary skilled in the art at the

time the invention was made to combine the teachings of Scoredos with the teachings

of Reddy in order to authenticate the remote user to access, monitor or execute the

application through monitoring software based on users build up profile kept in the

databases in appropriate domain.

5.   As to claim 12, Scoredos discloses, a system to filter server connections in an

embedded system, comprising:

a network interface to receive a connection request from a requestor (Fig.1, step-112, [0015, lines 13-14]), the connection request having an application layer connection component and a transport layer connection component ([0015, lines 1-4], tcp/ip connection means it contains header information which deals with transport layer and payload which contains data or deals with application layer.);

a filter device to filter connections using the transport layer connection component ([0015, line 14]), the filter device including a connection database and a throttle filter ([0015, lines 3-5], where firewall is filtering device and set of rules is a database), the connection database to store information about connection requests, the throttle filter having data from the connection database to filter connection requests using the transport layer connection component ([0016, lines 1-5], filtering, [0016, lines 1-4], table of rules could be a database); and

a controller coupled to the filter device and the network interface, the controller to apply the throttle filter to the transport layer connection component of the connection request, to drop the connection request silently if the throttle filter blocks the transport layer component, to proceed with an application layer connection if the throttle filter allows the transport layer component, to add data about the application layer connection to the connection database, and to update the throttle filter with information about the connection database (Fig.1, Step-112 and Step-101,[0015, lines 12-14], interface card is controller which is coupled with filtering device 101 and [0033, lines 2-4], where connection is dropped based on the limit rule and allowed packets will obviously be further processed).

Scoredos does not disclose explicitly, the connection database stores application

layer connection component outcomes. However, Reddy teaches, connection database

stores application layer connection component outcomes (Fig.2, Step-76, Col.6, lines

17-25 and lines 29-36, where database 76, keeps events which are outcomes of

application and uses them later on as web server sends the response to client through

HTTP protocol).

Therefore, it would have been obvious to one ordinary skilled in the art at the

time the invention was made to combine the teachings of Scoredos with the teachings

of Reddy in order to authenticate the remote user to access, monitor or execute the

application through monitoring software based on users build up profile kept in the

databases in appropriate domain.

6.   As to claim 27, a computer program product having a computer-readable

medium including computer program logic encoded thereon that, when performed on a

computer system directs the computer system to perform the method of:

receiving a connection request having an application layer component and

a transport layer component ([0015, lines 1-4], where tcp/ip connection comprises of

header information which is transport layer component and payload information which is

application layer component);

providing a connection database to store information about connection requests

[(0016, lines 1-4], table of rules is a database);

providing a throttle filter using data from the connection database, the throttle filter

to filter the connection request at the transport layer component ([0016, lines 1-5) and

[0050, lines 1-3], where limit rule is incorporated in the data structure);

applying the throttle filter to the received connection request ([0016, lines 7-9],

where packets are processed through filtering functions);

if the throttle filter blocks the transport layer component of the connection request,

dropping the connection request silently ([0033, lines 2-4]; depending on the rule

connection is dropped);

Scoredos does not explicitly disclose, providing a connection database to store

information about associated application layer outcomes; or if the throttle filter allows

the transport layer component of the connection request, proceeding with the

application layer component. However, Reddy teaches, providing a connection

database to store information of associated application layer outcomes (Col.7, lines 64-

66) ; and if the throttle filter allows the transport layer component of the connection

request, proceeding with the application layer component (Col.8, lines 5-23, where

notifications are outcome of applications outcome which are communicated through

firewall by web server and displayed at user interface in http form or could be a HTML

page with time out notice or error notice or status).

Therefore, it would have been obvious to one ordinary skilled in the art at the

time the invention was made to modify the teachings of Scoredos with the teachings of

Reddy in order to authenticate the remote user to access, monitor or execute the

application through monitoring software based on users build up profile kept in the

databases in appropriate domain.

7.   As to claim 2, Scoredos discloses, the method further comprising the steps of:

updating the throttle filter with information from the connection database (Fig.1,

Step-100, [0003, lines 5-10]).

Scoredos do not explicitly disclose, adding data from an application layer

outcome of the connection request to the connection database; However, Reddy

teaches, adding data from an application layer outcome of the connection request to

the connection database (Col.7, lines 64-66, where agent detects the application

outcome as notifications which is added into database Fig.2,Step-76);

Therefore, it would have been obvious to one ordinary skilled in the art at the

time the invention was made to modify the teachings of Scoredos with the teachings of

Reddy in order to authenticate the remote user to access, monitor or execute the

application through monitoring software based on users build up profile kept in the

databases in appropriate domain.

8.   As to claim 3, Scoredos discloses, the step of adding data comprises the steps

of:

recording a connection requestor identifier to the connection database ([0006, lines

7-9, where ip entity is connection requestor and ip is identifier); and

providing a connection requestor rank to the connection requestor identifier
([0057, lines 13-15], clearly shows that each connection has an ID against its
connection request) and [0059, lines 1-9], where hash technique is interpreted as
ranking to give priority for faster processing).

Scoredos does not explicitly teach, providing a connection requestor rank to the
connection requestor identifier based on an outcome of the application layer connection
component about application layer. However, Reddy teaches, the database adds all the
associated outcome events from each application and it will be an obvious variation to
construct some sort of ranking system to give priority to certain client entity based on
clients frequent request for certain application (Col.7, lines 64-66, where notifications
and events are the outcomes of applications running on compute, Fig.2, Step-40)

Therefore, it would have been obvious to one ordinary skilled in the art at the
time the invention was made to modify the teachings of Scoredos with the teachings of
Reddy in order to authenticate the remote user to access, monitor or execute the
application through monitoring software based on users build up profile kept in the
databases in appropriate domain.

9.   As to claim 5, Scoredos discloses, the method wherein, the throttle filter is a list
of connection request characteristics and the step of applying the throttle filter further
comprises comparing data from the connection request to the list of connection request
characteristics ([0006, lines 1-11], where limit table is interpreted as throttle filter).

10.   As to claim 6, Scoredos discloses, the method wherein, the list of connection request characteristics further comprises a list of connection requestor IP addresses to be blocked as indicated by data from the connection database ([0002, lines 7-11], where set of rules is a database and set of rules can be a list of blocked IP addresses).

11.   As to claim 7, Scoredos discloses, the method wherein, the list of connection request characteristics further comprises a list of connection requestor port numbers to be blocked as indicated by data from the connection database ([0002, lines 7-11], where set of rules is a database and set of rules can be a list of blocked ip addresses and each IP carries a port number in the header information).

12.   As to claim 8, Scoredos discloses, the method wherein, the list of connection request characteristics further comprises a list of connection requestor virtual routing forwarding table IDs to be blocked as indicated by data from the connection database ([0016, lines 1-5], where destination IP can be a VRF ID which has an entry in State table in the database and [0003, lines 3-4, where it is acknowledged that rules can be programmed to block specific addresses).

13.   As to claim 10, Scoredos discloses, the method wherein the connection request is an HTTP request, the transport layer component is TCP connection component ([0015, lines 10-14]).

Scoredos does not disclose explicitly, the application layer component is an

HTTP connection component. However, Reddy teaches, the application layer

component is an HTTP connection component (Col.8, lines 46-49).

Therefore, it would have been obvious to one ordinary skilled in the art at the

time the invention was made to modify the teachings of Scoredos with the teachings of

Reddy in order to authenticate the remote user to access, monitor or execute the

application through monitoring software based on users build up profile kept in the

databases in appropriate domain.

14.   As to claim 11, 13 and 14, the claims are rejected for the same reasons set forth

in claim 10 above.

15.   As to claim 15, Scoredos discloses, the system wherein the filter device further

comprises a rate limiter to switch the filter device between global and selective modes

(0052, lines 5-9, where limit table is rate limiter and allowed or blocked states are global

and selective modes), the rate limiter to switch the filter device to global mode if a rate

limit threshold is exceeded and to switch the filter device to selective mode if the rate

limit threshold is not exceeded (Fig.1, Step-112, [0052, lines 10-14], where limit table is

a rate limiter and if connection establishes or allowed it is a selective mode if connection

is blocked it can be interpret as selective mode)

the controller configured to drop the connection request silently without applying

the throttle filter if the filter device is in global mode and to apply the throttle filter if the

filter device is in selective mode (Fig.1, Step-123 [0016, lines 5-6], where, switch is

controller to forward or drop the connection).

16.   As to claim 16, Scoredos discloses, the system wherein the rate limit threshold

further comprises a limit of connections created in a connection cycle period ([0046,

lines 4-6]).

17.   As to claim 17, Scoredos discloses, the system wherein the rate limit threshold

further comprises a rate of incoming connections ([0052, lines 1-9]).

18.   As to claim 18, Scoredos discloses, the system wherein the connection database

is a table in which each entry has an IP address of a connection requestor and an

associated rank based on an outcome of a connection attempted in response to a

connection request from the connection requestor ([0050, lines 1-4], database create an

entry of every connection and [0053, lines 1-9], connection is prioritized based on prior

entry and connection history in the database).

19.   As to claim 19, Scoredos discloses, the system wherein each entry of the table

further includes a port number of the connection requestor ([0053, lines 5-9], where

database also keeps an entry of connection port number).

20.   As to claim 20, Scoredos discloses, the system wherein each entry of the table

further includes a virtual routing forwarding table ID of the connection requestor ([0053,

liens 1-5], where state table entry can be a VRF pointer assigned to each connection

attempted at application layer).

21.   As to claim 22, Scoredos discloses, the system wherein the throttle filter is a list

of IP addresses of connection requestors to be blocked as indicated by data from the

connection database ([0047, lines 1-22], where limit table keeps all the matching source

IP, port and destination IP information which are allowable IP's).

22.   As to claim 23, Scoredos discloses, the system wherein the throttle filter further

includes port numbers of connection requestors to be blocked as indicated by data from

the connection database ([0047, lines 1-22], where limit table keeps all the matching

source IP, port and destination IP information which are allowable IP's).

23.   As to claim 24, Scoredos discloses, the system wherein the throttle filter further

includes virtual routing forwarding table IDs of connection requestors to be blocked as

indicated by data from the connection database ([0053, lines 9-12], where special type

of rule is created for group of IP addresses which comply with the limit rule, so they can

be allowable at next connection instead of getting blocked).

24.   Claim 9 is rejected under 35 U.S.C 103 as being unpatentable over Scoredos in

view of Reddy and further in view of Maruyama et al. (Pub. No.: US 2002/0124103 A1),

hereinafter, "Maruyama".

25.   As to claim 9, Scoredos discloses, a method wherein the step of applying the

throttle filter further comprises the steps of:

determining whether a limit of connections created in a connection cycle period

has been exceeded ([0033, lines 1-2], where rule is set to check the connections per IP

address);

if the limit of connections created has been exceeded, dropping the connection

request ([0033, lines 2-4], where exceeded connection is dropped);

neither Scoredos nor Reddy explicitly discloses, if the limit of connections

created has not been exceeded, determining whether a rate of incoming connections

has been exceeded or if the rate of incoming connections has been exceeded, then

dropping the connection request silently or if the rate of incoming connections has not

been exceeded, then comparing requestor identification information in the TCP

connection component of the connection request to data in the throttle filter. However,

Maruyama teaches, if the limit of connections created has not been exceeded,

determining whether a rate of incoming connections has been exceeded ([0011, lines

10-20], TCP connection rate is monitored for security purposes). Maruyama also

discloses, if the rate of incoming connections has been exceeded, then dropping the

connection request silently ([0011,lines 24-28], where excessive connection is dropped).

Maruyama further discloses, if the rate of incoming connections has not been exceeded, then comparing requestor identification information in the TCP connection component of the connection request to data in the throttle filter ([0035, 16-22], where identifier in the tcp packet is examined whether to allow a new connection or associate with established connection).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the teachings of Scoredos, and Reddy with the teachings of Maruyama in order to establish a monitoring system from remote computer to keep track of working applications by anticipating the critical notifications/outcomes generated by those applications and associated solutions to these outcomes.

26.   Claims 25 and 26 are rejected under 35 U.S.C 103 as being unpatentable over Scoredos in view of Maruyama and further in view of Reddy.

27.   As to claim 25, Scoredos discloses, a method for filtering HTTP server connections in an embedded system, comprising the steps of:

receiving a connection request having an HTTP connection component and a TCP connection component ([0015, lines 1-4], where header information in the packet is TCP connection and payload data is an http connection);

providing a connection database to store information about connection requests ([0016, lines 1-4], table of rules can be a database);

providing a throttle filter using data from the connection database, the throttle filter

to filter the connection request at the TCP connection component ([0016, lines 1-5],

where switch-123 is a throttle filter);

if the limit of connections created has not been exceeded ([0033, lines 1-2],

where connection status can show if the limit has exceeded);

determining whether a limit of connections created in a connection cycle period

has been exceeded ([0033, lines 1-2], where rule has defined for maximum connection

in limit rule also where rule is set to check the connections per IP address);

if the limit of connections created has been exceeded, dropping the connection

request silently (0033, lines 2-4], where exceeded connection is dropped);

if the throttle filter blocks the TCP connection component, dropping the

connection request silently ([0033, lines 2-4]);

updating the throttle filter with information from the connection database

([0052, lines 10-12]).

Scoredos do not explicitly discloses, if the limit of connections created has not

been exceeded, determining whether a rate of incoming connections has been

exceeded or if the rate of incoming connections has been exceeded, then dropping the

connection request silently or if the rate of incoming connections has not been

exceeded, then comparing requestor identification information in the TCP connection

component of the connection request to data in the throttle filter or adding data from the

HTTP connection component to the connection database. However, Maruyama

teaches, if the limit of connections created has not been exceeded, determining whether

a rate of incoming connections has been exceeded ([0011, lines 10-20], tcp connection

rate is monitored for security purposes). Maruyama also discloses, if the rate of

incoming connections has been exceeded, then dropping the connection request

silently ([0011,lines 24-28, where excessive connection is dropped). Maruyama further

discloses, if the rate of incoming connections has not been exceeded, then comparing

requestor identification information in the TCP connection component of the connection

request to data in the throttle filter ([0035, 16-22], where identifier in the tcp packet is

examined whether to allow a new connection or associate with established connection).

Neither Scoredos nor Maruyama discloses, if the throttle filter allows the TCP

connection component, proceeding with the HTTP connection component or adding

data from the HTTP connection component to the connection database. However,

Reddy discloses, if the throttle filter allows the TCP connection component, proceeding

with the HTTP connection component (Col.7, lines 41-45, where user has established

the http connection). Reddy further discloses, adding data from the HTTP connection

component to the connection database (Col.7, lines 41-48 and lines 4-7, where it can be

seen that user's HTTP request has to go through security Fig.2, step-86 where his login

will be added into security database).

Therefore, it would have been obvious to one ordinary skilled in the art at the

time the invention was made to modify the teachings of Scoredos and Maruyama with

the teachings of Reddy in order to establish a monitoring system from remote computer

to keep track of working applications by anticipating the critical notifications/outcomes

generated by those applications and associated solutions to these outcomes.

28.   As to claim 26, Scoredos discloses, a method for filtering HTTPS server

connections in an embedded system, comprising the steps of:

receiving a connection request having an HTTPS connection component and a

TCP connection component ([0015, lines 1-4], TCP header information is a transport

layer component and payload is a HTTPS component);

providing a connection database to store information about connection requests

([0016, lines 1-4], table of rules can be a database);

providing a throttle filter using data from the connection database, the throttle

filter to filter the connection request at the TCP connection component (Fig.1, step-123,

[0016, lines 1-5], where switch is a throttle filter which filters the connections);

determining whether a limit of connections created in a connection cycle period

has been exceeded ([0033, lines 1-2], where rule is set to check the connections per IP

address);

if the limit of connections created has been exceeded, dropping the connection

request silently (0033, lines 2-4], where exceeded connection is dropped);

if the throttle filter blocks the TCP connection component, dropping the

connection request silently ([000052, lines 13-14], where connection can be dropped

silently or reset based on the specified rule);

if the throttle filter allows the TCP connection component, proceeding with the

HTTPS connection component (Col.7, lines 41-45, where user has established the http

connection);

updating the throttle filter with information from the connection database ([0052,

lines 10-12]).

Scoredos do not explicitly discloses, if the limit of connections created has not been

exceeded, determining whether a rate of incoming connections has been exceeded or if

the rate of incoming connections has been exceeded, then dropping the connection

request silently or if the rate of incoming connections has not been exceeded, then

comparing requestor identification information in the TCP connection component of the

connection request to data in the throttle filter. However, Maruyama teaches, if the limit

of connections created has not been exceeded, determining whether a rate of incoming

connections has been exceeded ([0011, lines 10-20], TCP connection rate is monitored

for security purposes). Maruyama also discloses, if the rate of incoming connections

has been exceeded, then dropping the connection request silently ([0011,lines 24-28,

where excessive connection is dropped). Maruyama further discloses, if the rate of

incoming connections has not been exceeded, then comparing requestor identification

information in the TCP connection component of the connection request to data in the

throttle filter ([0035, 16-22], where identifier in the tcp packet is examined whether to

allow a new connection or associate with established connection). Neither Scoredos nor

Maruyama discloses, if the throttle filter allows the TCP connection component,

proceeding with the HTTP connection component or adding data from the HTTP

connection component to the connection database. However, Reddy discloses, if the

throttle filter allows the TCP connection component, proceeding with the HTTP

connection component (Col.7, lines 41-45, where user has established the http

connection). Reddy further discloses, adding data from the HTTP connection

component to the connection database (Col.7, lines 41-48 and lines 4-7, where it can be

seen that user's HTTP request has to go through security Fig.2, step-86 where his login

will be added into security database).

Therefore, it would have been obvious to one ordinary skilled in the art at the

time the invention was made to modify the teachings of Scoredos and Maruyama with

the teachings of Reddy in order to establish a monitoring system from remote computer

to keep track of working applications by anticipating the critical notifications/outcomes

generated by those applications and associated solutions to these outcomes.

29.   Claim 4 and 21 are rejected under 35 U.S.C 103 as being unpatentable over

Scoredos in view of Reddy and further in view of Gillies et al. (Pub No.: US

2003/0212821 A1), hereinafter "Gillies".

30.   As to claim 4, neither Scoredos nor Reddy discloses, the method wherein the

step of updating the throttle filter with information from the connection database

comprises periodically replacing throttle filter data with a preselected number of

connection requestor identifiers ranked least desirable in the connection database.

However, Gillies teaches, updating the throttle filter with information from the

connection database comprises periodically replacing throttle filter data with a

preselected number of connection requestor identifiers ranked least (Fig. 6E, [0093,

lines 4-16], where data is getting replaced by age and old data is getting replaced by new data periodically).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the teachings of Scoredos and Reddy with the teachings of Gillies in order to update the data and discard old data with newer data in order to control the size of the database and avoid the multiplicity of same data.

31.   As to claim 21, neither Scoredos nor Reddy discloses the system wherein each entry in the table includes an entry age, the filter device configured to delete entries having an entry age that exceeds an age threshold.

However, Gillies teaches, wherein each entry in the table includes an entry age, the filter device configured to delete entries having an entry age that exceeds an age threshold (Fig. 6E, [0093, lines 4-16], where data is getting replaced by age and old data is getting replaced by new data periodically).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the teachings of Scoredos and Reddy with the teachings of Gillies in order to update the data and discard old data with newer data in order to control the size of the database and avoid the multiplicity of same data.

Conclusion

32.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Le et al. (US 20006/02423313 A1) discloses, packet receiver over the network is routed using a packet engine.

Muller et al. (US 6650640) discloses, flow of packets from source to destination.

Mawhinney et al. (US 6826620) discloses, network congestion control system and method to control the flow of packet to a point where packets where network has to discard data.

Donahue (US 2006/0256788 A1) discloses, system and method through content filtering router.

33.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tauqir Hussain whose telephone number is 571-272-1247. The examiner can normally be reached on 7:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nabil El Hady can be reached on 571 272 3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TH

ANDREW Y. KOENIG
PRIMARY PATENT EXAMINER